RSAC 2025 Conference

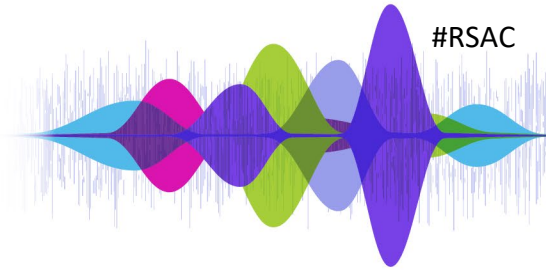
Many Voices.
One Community.

SESSION ID: DSA-R05

Protect that Money Maker: Product Security Patterns and Practices

Stirling Goetz
Cybersecurity Executive
Pixel Fire
https://linkedin.com/in/stirlinggoetz

Geoffrey Hill
Founder and Inventor
Tutamantic_Sec
https://linkedin.com/in/geoffrey-hill-tutamantic



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Information presented is for informational purposes only. The speakers assume no liability for any errors, omissions, or inaccuracies in the content, nor for any actions taken based on this information. Views expressed are solely those of the speakers and do not represent the views of their employers or affiliated organizations. Every product security program is unique; please contextualize any information presented here to your specific environment before application.

RSAC 2025 Conference

“If you're faced with the tradeoff between security and another priority, your answer is clear: Do security.”

- Satya Nadella

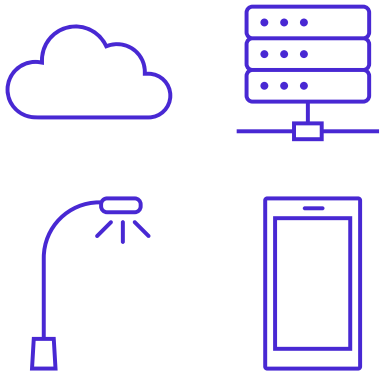
Many Voices.
One Community.

Definitions for this Session

- **Digital products** process, communicate, and generate revenue
  - Smart speaker, connected medical device, connected car, SaaS, etc.
- **Product security** integrates security across the product portfolio
  - Goals include: Protect those who buy and use products, protect product revenue, reduce lifecycle costs, **increase product value.**

Isn’t Product Security Just <Topic X>?

- Product vendors **make** products and enterprises **adopt** products
- Product security focus is different than enterprise security and requires unique role expertise
  - E.g. New feature ideation, secure manufacturing, engineering system integration, end-of-life
  - Technologist, R&D knowledge, product lifecycles, evangelism, educator, culture changer, influencer

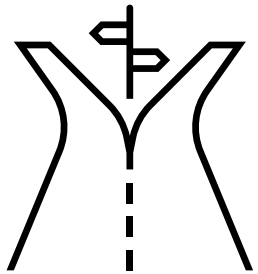


Why should we care?

- Shift left and accelerate
- Automate security activities
- Leverage security for differentiation

Champions

- Speed to market
- Innovation time regained
- Increase prod value



Underperformers

- Public scrutiny
- Lost sales
- Governmental fines

- Potential TP-Link market ban after US Commerce, Defense, Justice and Congress attention
- EU Cyber Resilience Act €15M or 2.5%

Amplifying Trends

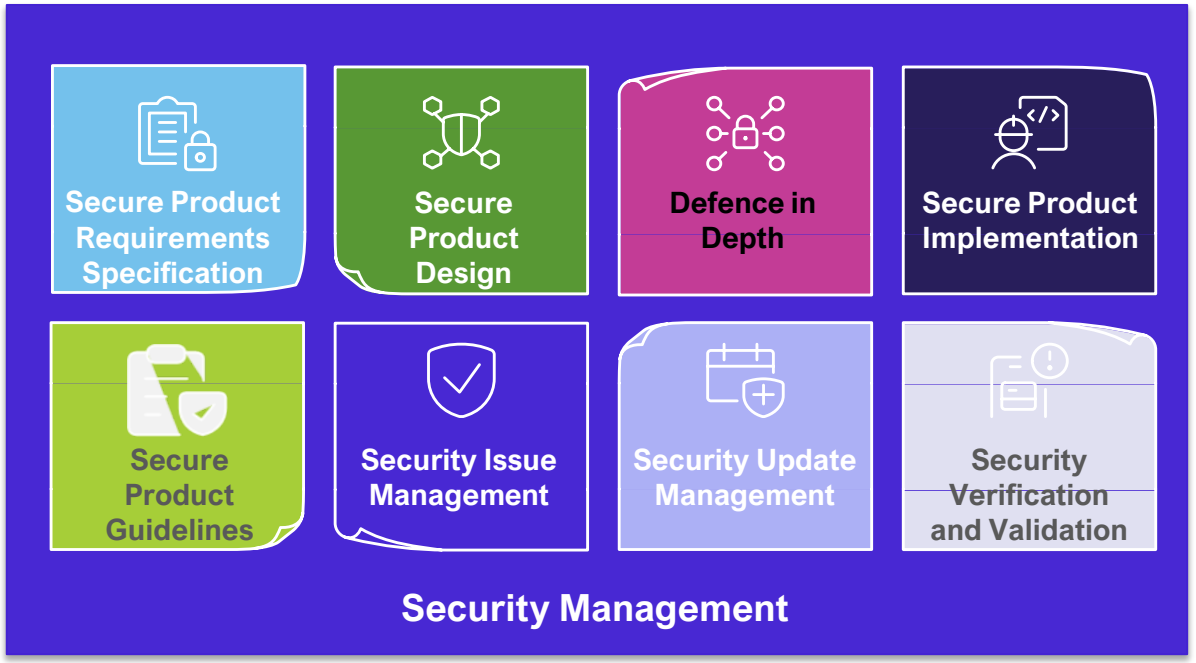
Growing transparency need	Industry knowledge gap	Growing supply chain attacks	Underserved platform support	Product retirement challenges

PIXEL FIRE

Guidance Varies By Product and Industry

- Industrial Automation and Control
  - IEC 62443
- Automotive
  - ISO 21434
- Medical
  - Regulations, Standards, Guidelines
- Cyber Hygiene
  - Consumer IOT guidelines
- Other guidance
  - Secure SDLC: e.g. SafeCode, NIST SSDF
  - Comprehensive: e.g. NIST CSF, ISO 27001

Sample Product Security Guidance Domains



Leverage Valuable Aspects From IACS

Security Role Responsibilities

Highlights responsibilities in operationally complex products

Product Security Levels

Allows for risk-based scalability of security focus. Consider for healthcare, government, telecom

Secure Development Lifecycle

Supports secure development for embedded systems and IoT

Defense in Depth

Emphasizes layered security which is applicable to virtually all industries

Availability & Safety

Ensures principles of availability and safety in sectors like transportation and mining.

IEC 62443

PIXEL FIRE

RSAC 2025 Conference

Leveraging Valuable Aspects From Automotive

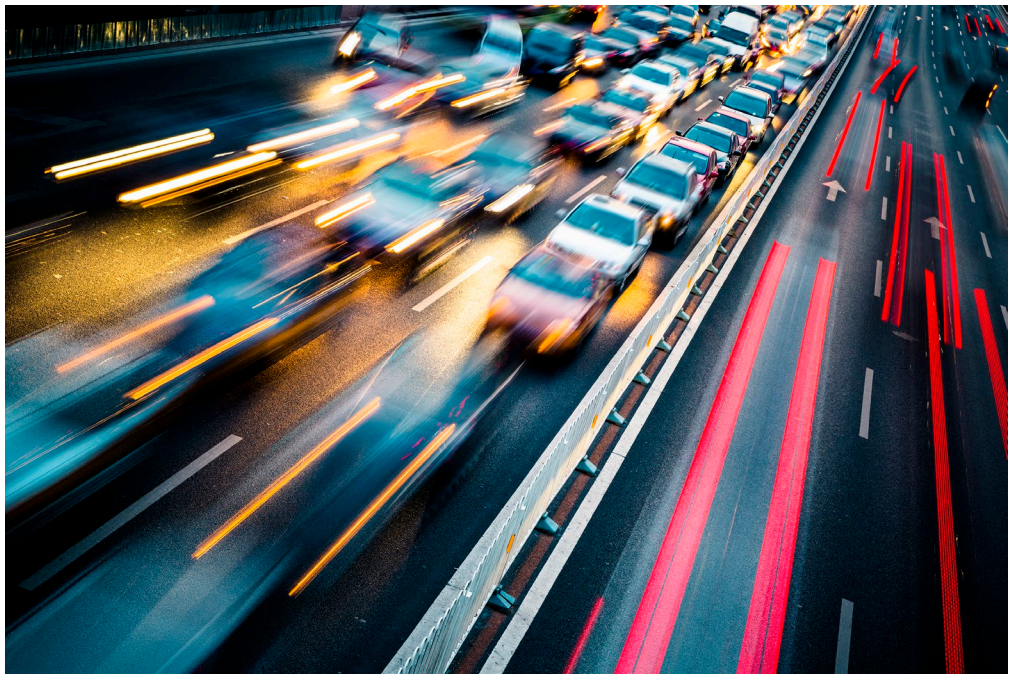
Safety-Criticality
Consider for aerospace, rail transportation, industrial robotics

Long Lifecycles
Consider for industrial equipment, medical devices

Complex Supply Chains
Consider for defense, pharmaceuticals, large-scale manufacturing

Regulatory Compliance
Consider for medical devices, aviation, rail

Complex Threat Modeling
Consider for smart grids, smart buildings



ISO 21434

PIXEL FIRE

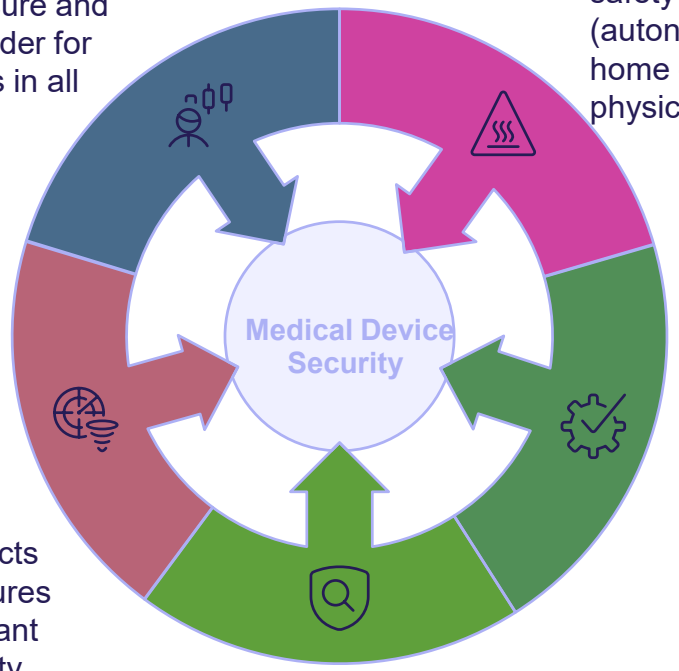
Leveraging Valuable Aspects From Medical

Post-Market

Surveillance, updates, vulnerability disclosure and coordination. Consider for connected products in all industries

Physical Harm Potential

Consider for products with safety-critical features (autonomous vehicles, smart home devices controlling physical access)



Threat Modeling Focus on Real-world Impact.

Consider for products where security failures could have significant operational or safety implications.

Functionality & Reliability with Security Constraints

Consider for cloud services, industrial automation

Rigorous Security Review in Approval and Release

Consider for addressing vulnerabilities earlier across industries

Regulations, Standards, Guidelines

Minimum Viable Security: Plan for Compliance (IOT)

NP No Default Passwords	**VD** • Vulnerability Disclosure	**SU** • Secure Updates	**SS** • Secure Storage	**SC** • Secure Communication	**MA** • Minimize Attack Surface
SI • Software Integrity	**DP** • Data Protection	**RR** • Resilience to Outages	**EL** • Event Logging	**DD** • Data Deletion	**EI** • Easy Installation
IV • Input Validation	**DI** • Device Identification	**DC** • Device Configuration	**LA** • Logical Access	**IE** • Insecure Ecosystem	**IO** • Insecure/Outdated Components
	DM • Device Management	**DS** • Default Settings	**PH** • Physical Hardening	**RS** • Reasonable Security	

ETSI EN 303 645 | NIST IR 8259A | OWASP IoT Top 10 | UK CoP for Consumer IoT Sec | California SB-327 | Singapore Cyber Sec Labelling (CLS) | AU CoP: Securing Consumer IoT

PIXEL FIRE

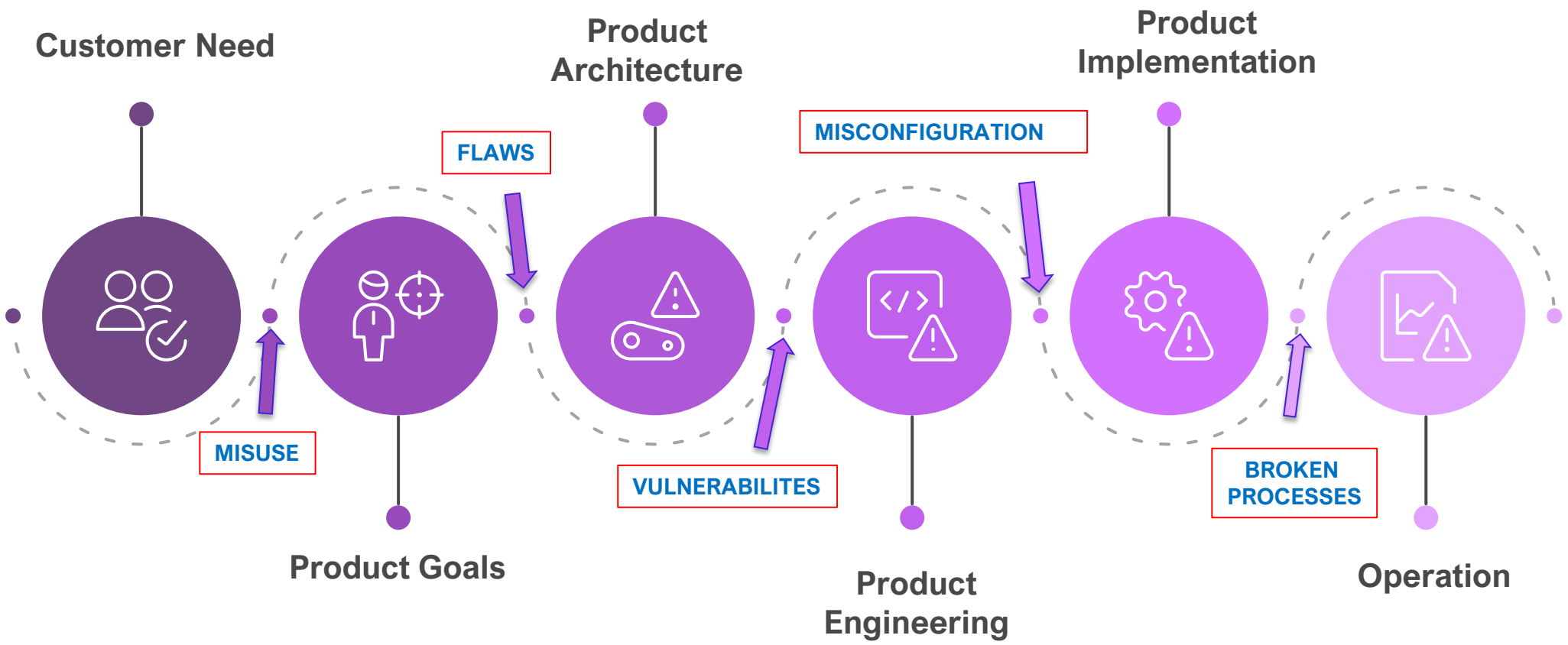
Minimum Viable Security: Plan For Threats (ICS)

ICS 5 Critical Controls	Vendor Actions	Supporting Product Features/Processes
ICS Incident Response Plan	Enable Forensic Readiness & Response Support:	• Comprehensive/Exportable Logs (NTP sync) • Provide Log Docs & Config Guides • Establish PSIRT for Support • Document Incident Reporting
Defensible Architecture	Build Secure and Segmentable Products	• Document Network Needs (Ports/Protocols) • Implement RBAC / Least Privilege • Use Secure Protocols; Secure Coding (SDLC) • Provide Hardening Guides
ICS Network Visibility & Monitoring	Design for Monitorability	• Design for Monitorability (Logs, Standard Logging Protocols) • Document "Normal" Baselines & Indicators • Minimize Obscure Protocols • Implement Health Status Monitoring
Secure Remote Access	Implement & Guide Secure Access Methods	• Support Secure Auth (MFA) • Enforce Strong Credential Policies (No Defaults) • Implement/Guide Secure Channels (SSH/TLS, VPN) • Enforce RBAC / Least Privilege • Log Remote Access; Provide Config Guidance
Risk-Based Vulnerability Management	Establish a Mature Vulnerability Management Lifecycle	• Implement Secure Dev Lifecycle (SDL): Threat Model, Test • Establish PSIRT • Develop & Publish SBOMs • Provide Timely Patches & Advisories (CSAF/VEX) • Guide on Compensating Controls

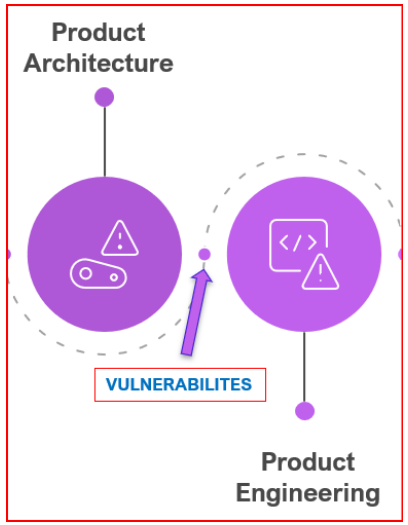
PIXEL FIRE

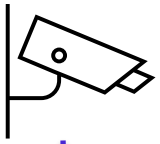
*https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls

Product Security Pitfall Genesis



Product Security In The News





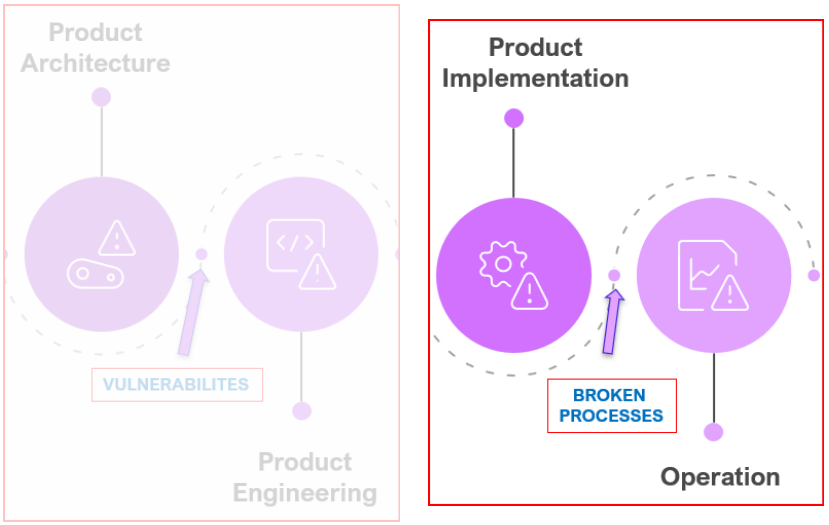
AVTECH AVM1203 0-Day

Issue: CMD injection
Fix: Proactive EoL Process

2024

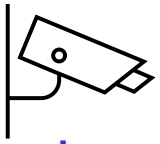
2025

Product Security In The News



Secure Product Implementation

Secure Product Guidelines

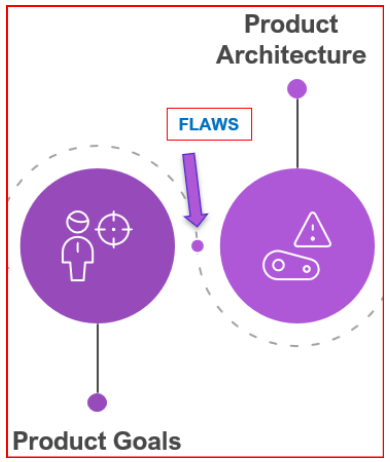


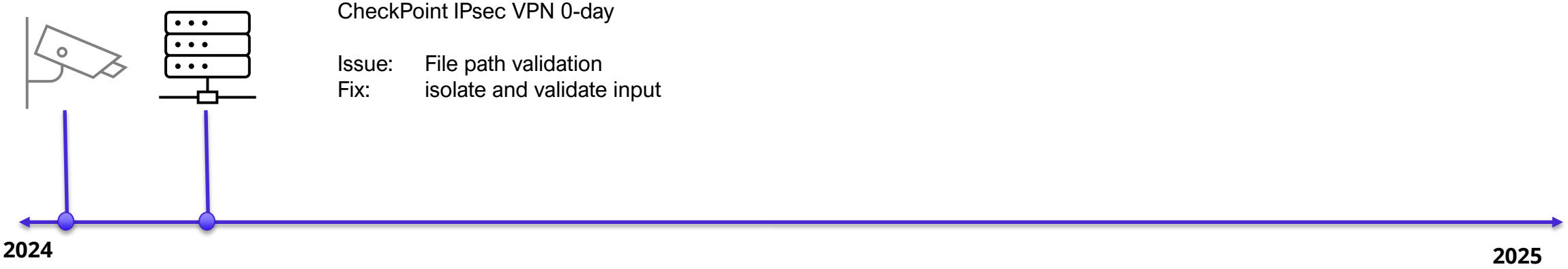
AVTECH AVM1203 0-Day

Issue: CMD injection
Fix: Proactive EoL Process

2024 — **2025**

Product Security In The News

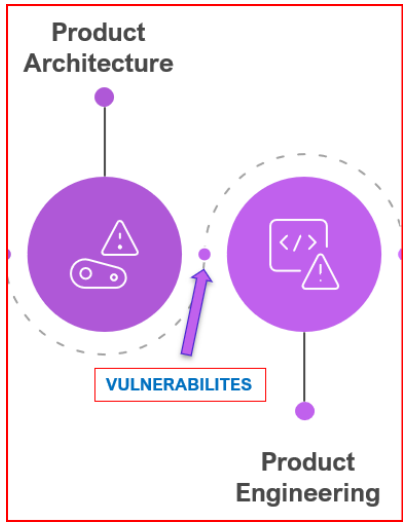


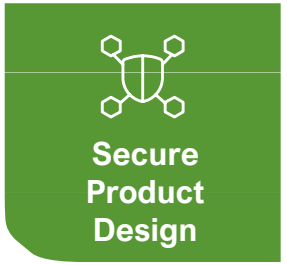


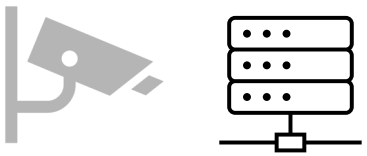
CheckPoint IPsec VPN 0-day

Issue: File path validation
Fix: isolate and validate input

Product Security In The News



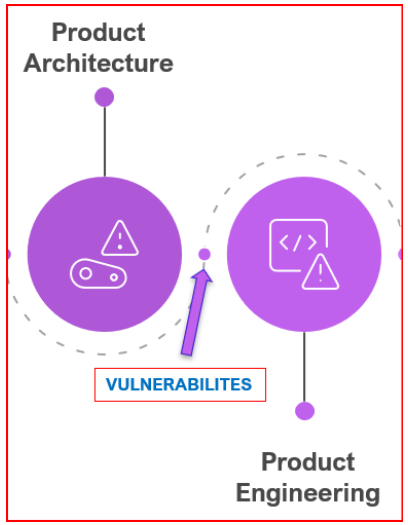


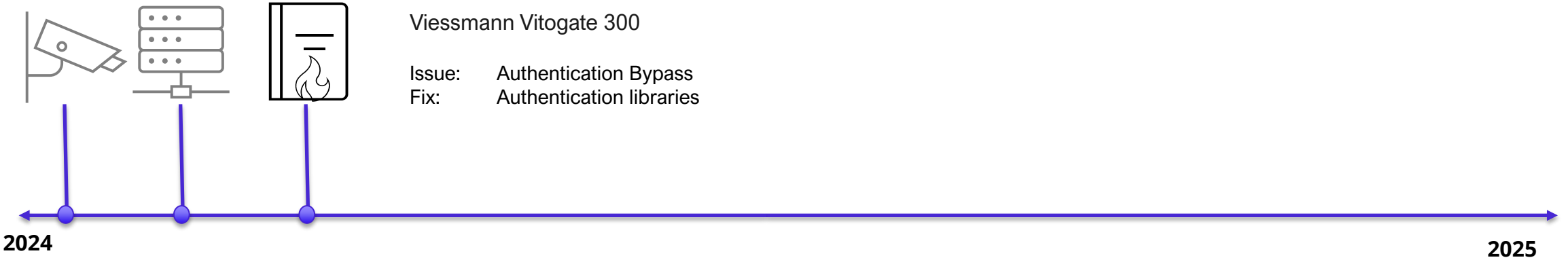


CheckPoint IPsec VPN 0-day

Issue: File path validation
Fix: isolate and validate input

Product Security In The News



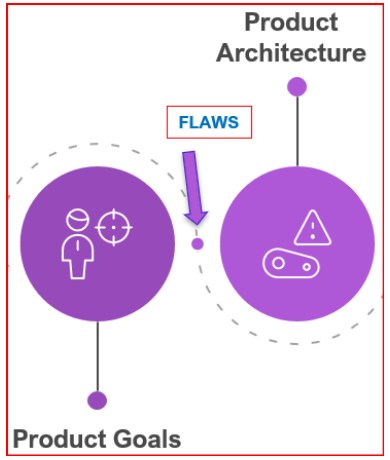


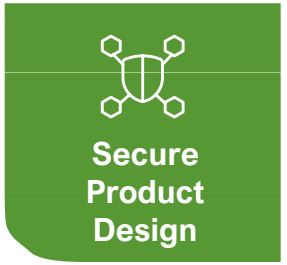
Viessmann Vitogate 300

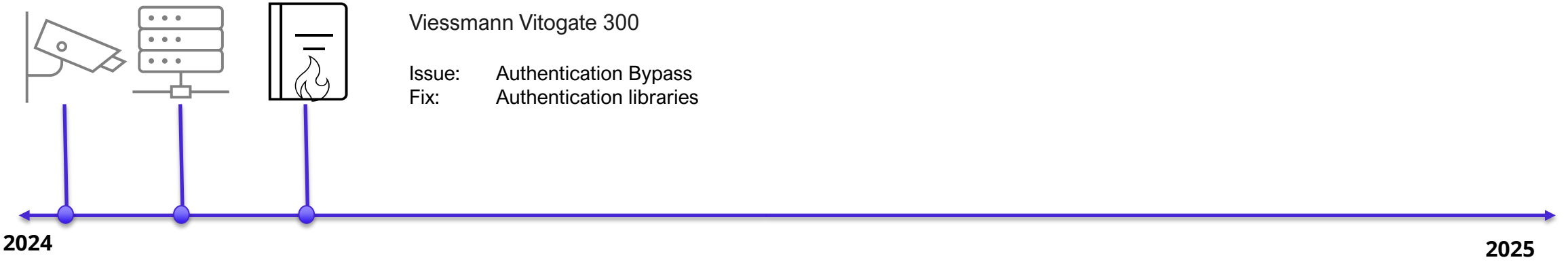
Issue: Authentication Bypass
Fix: Authentication libraries

PIXEL FIRE
RSAC 2025 Conference

Product Security In The News



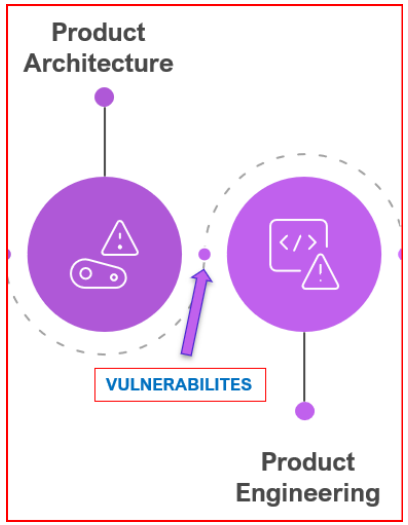




Viessmann Vitogate 300

Issue: Authentication Bypass
Fix: Authentication libraries

Product Security In The News



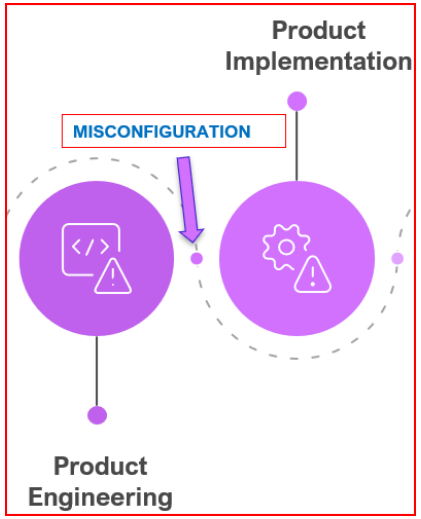
Contec Health CMS8000 Patient Monitor

Issue: Hardcoded IPs
Fix: Product secure by default

Product Security In The News

Secure Product Requirements Specification

Secure Product Implementation



Contec Health CMS8000 Patient Monitor

Issue: Hardcoded IPs
Fix: Product secure by default

Energy Products

Challenges
- Portfolio coverage
- Limited talent
- Security incentives, culture and knowledge
- Growing product connectivity

Practice improvements

Leadership and governance	[Security Mgt]
Portfolio risk targeting	[Security Mgt]
Automation and champions	[Implementation]
Security concepting for value	[Sec Prod Design]

Medical Device Products

Challenges
- Product management disconnect
- Long development cycles
- Supply chain risks

Practice improvements

Cross-org comms	[Security Mgt]
Modernizing product dev/eng	[Design and Impl]
Upstream supplier mandates	[Security Mgt]
Industry specific methods	[Sec Product Req]

PIXEL FIRE
RSAC 2025 Conference

Crypto Asset Storage Product

Challenges
- Supply chain security gaps
- Lack of central security authority
- Security not in design / implementation / verification

Practice Improvements
- Supply chain [Security Guidelines]
- **Governance** [Security Mgt]
- Central security group [Security Mgt]
- Secure patterns library [Secure By Design]

Money Transfer Product

Challenges
- Weak authentication / poor MFA
- No secure architecture, no physical security
- Security not a priority / lack of training

Practice Improvements
- Authentication patterns [Secure Requirements]
- Additional threat modeling [Secure By Design]
- Security awareness [Security Guidelines]
- **Security champions** [Security Guidelines]

PIXEL FIRE

Reoccurring Program Themes

Organizational Responsibility

Varies based on organizational structure, culture, and industry

Enterprise Security Maturity

Varying suitability of enterprise security capabilities for product security lifecycles

Legacy Methods Impact

Slow development and engineering approaches Introducing security risks

Security Engagement Timing

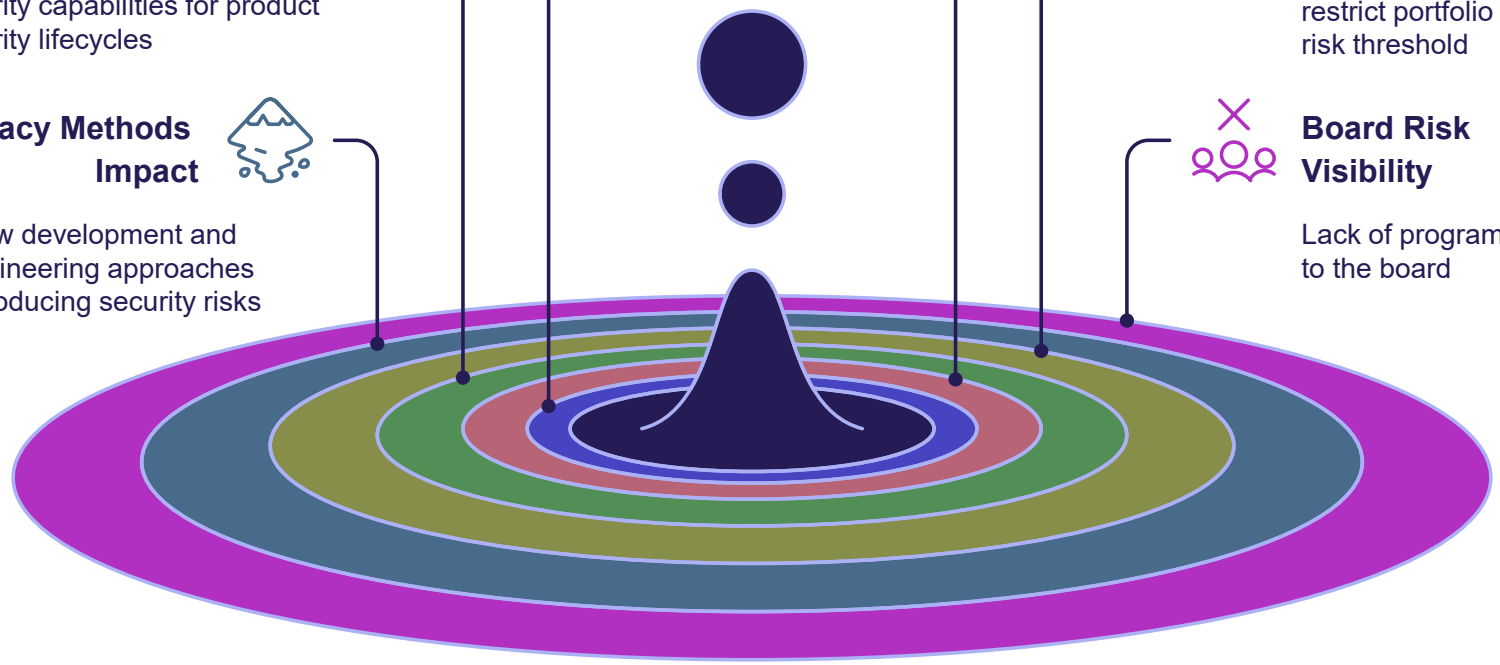
Security brought in during design or verification and validation

Team Scaling Issues

Talent and budget limitations restrict portfolio attention below risk threshold

Board Risk Visibility

Lack of program status reporting to the board



PIXEL FIRE

RSAC 2025 Conference

Moving the Maturity Needle - Overview

Business Function	***Level 1: Foundational***	***Level 2: Defined***	***Level 3: Measured***	***Level 4: Optimized***
Governance	Basic Awareness, Informal Activities	**Named Lead**, Policy Defined, **Exec Sponsor**, **Initial Budget,** Awareness Training, **Coalition Building,** Basic Assurance, Initial Procurement Req	**Executive Mandate**, Formal Program (PSO), **Role-Based Training**, Metrics, Portfolio Risk Mgmt, Formal Budget, 3rd Party Risk Mgmt	**Pervasive Security Culture**, Predictive Metrics, Automated Compliance, **Perf. Goals,** Dynamic Budget, Advanced Supply Chain Sec
Design	Informal Consideration, Basic Checklists	**Basic Threat Modeling** (Critical), **Req. Processes & Objectives**	**Secure by Design (**Integrated Threat Modeling, Arch Reviews, Formal Req), **Security Feature Planning**, Initial Accessibility	**Continuous Threat Modeling** (Intel-fed), Int Resilient Arch Patterns, Dynamic Req, **Resilient Design**
Implementation	Ad-hoc Secure Coding, Informal Reviews	Documented Standards, Security in Code Review, Basic SAST/DAST/SCA	Enforced Standards, **Basic Security Management Platform**, Integrated SAST/DAST/SCA	**Automated Secure Product Pipeline** (Incl DevSecOps, IAST), Self-Service Platform
Verification	Limited Ad-hoc Testing	Intro SAST, **Basic QA Security Tests**, Vuln Triage	Regular Pen Testing, Integrated QA Security, **Vuln Mgmt**	Comprehensive Automated Testing (Incl Fuzz), Continuous Pen Test, **Purple Teaming**, Bug Bounty
Operations	Reactive Vuln Handling	**Defined CVD Policy & Intake**, Basic Patching, Basic Docs	Mature CVD (SLAs), **PSIRT Established**, **Timely Patching**, Customer Bulletins/SBOMs	Proactive Security Research, **Efficient PSIRT** (Automation), Auto-Patching (Opt), **Cont Monitor**

PIXEL FIRE

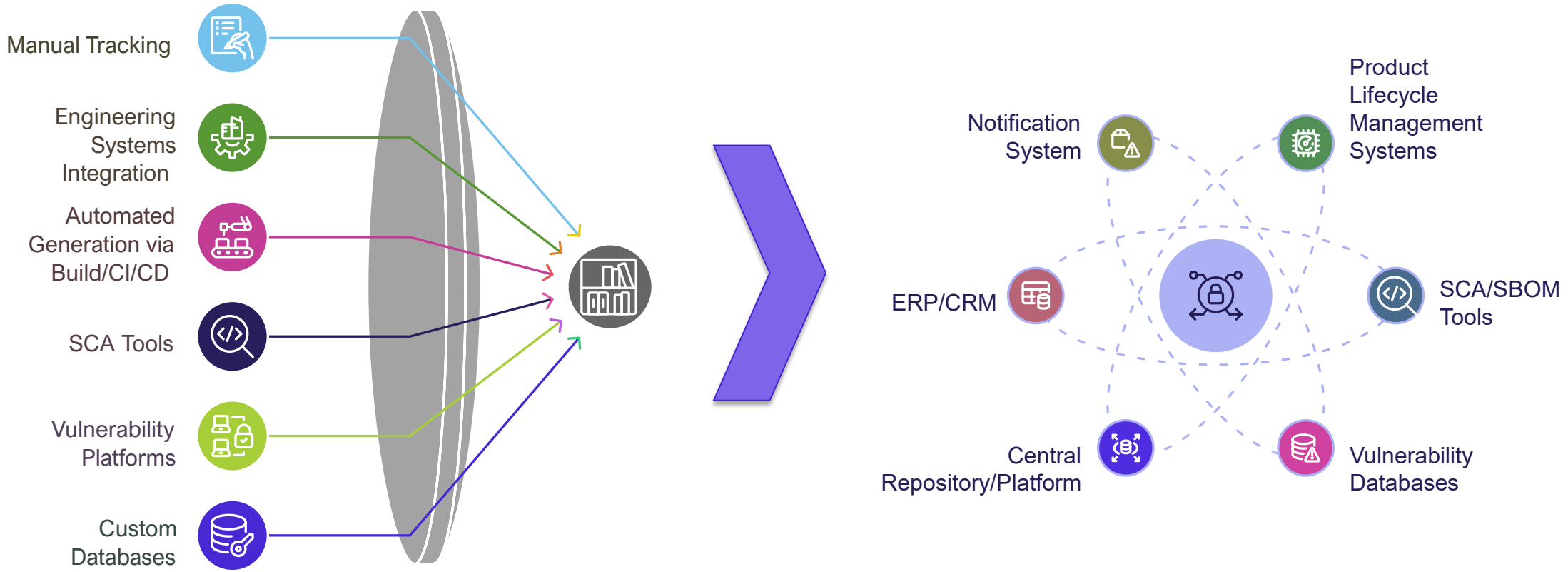
Moving the Maturity Needle – Early (L1 & L2)

Business Function	***Level 1: Foundational***	***Level 2: Defined***
Governance	Basic Awareness, Informal Activities	**Named Lead**, Policy Defined, **Exec Sponsor**, **Initial Budget,** Awareness Training, **Coalition Building,** Basic Assurance, Initial Procurement Req
Design	Informal Consideration, Basic Checklists	**Basic Threat Modeling** (Critical), **Req. Processes & Objectives**
Implementation	Ad-hoc Secure Coding, Informal Reviews	Documented Standards, Security in Code Review, Basic SAST/DAST/SCA
Verification	Limited Ad-hoc Testing	Intro SAST, **Basic QA Security Tests**, Vuln Triage
Operations	Reactive Vuln Handling	**Defined CVD Policy & Intake**, Basic Patching, Basic Docs

Moving the Maturity Needle – Late (L3 & L4)

Business Function	***Level 3: Measured***	***Level 4: Optimized***
Governance	**Executive Mandate**, Formal Program (PSO), **Role-Based Training**, Metrics, Portfolio Risk Mgmt, Formal Budget, 3rd Party Risk Mgmt	**Pervasive Security Culture**, Predictive Metrics, Automated Compliance, Perf Goals, Dynamic Budget, Advanced Supply Chain Sec
Design	**Secure by Design** (Integrated Threat Modeling, Arch Reviews, Formal Req), **Security Feature Planning**, Initial Accessibility	**Continuous Threat Modeling** (**Intel-fed**), Int Resilient Arch Patterns, Dynamic Req, **Resilient Design**
Implementation	Enforced Standards, **Basic Security Management Platform**, Integrated SAST/DAST/SCA	**Automated Secure Product Pipeline** (Incl DevSecOps, IAST), Self-Service Platform
Verification	Regular Pen Testing, Integrated QA Security, **Vuln Mgmt**	Comprehensive Automated Testing (Incl Fuzz), Continuous Pen Test, **Purple Teaming**, Bug Bounty
Operations	Mature CVD (SLAs), **PSIRT Established**, **Timely Patching**, Customer Bulletins/SBOMs	Proactive Security Research, **Efficient PSIRT** (Automation), Auto-Patching (Opt), **Cont Monitor**

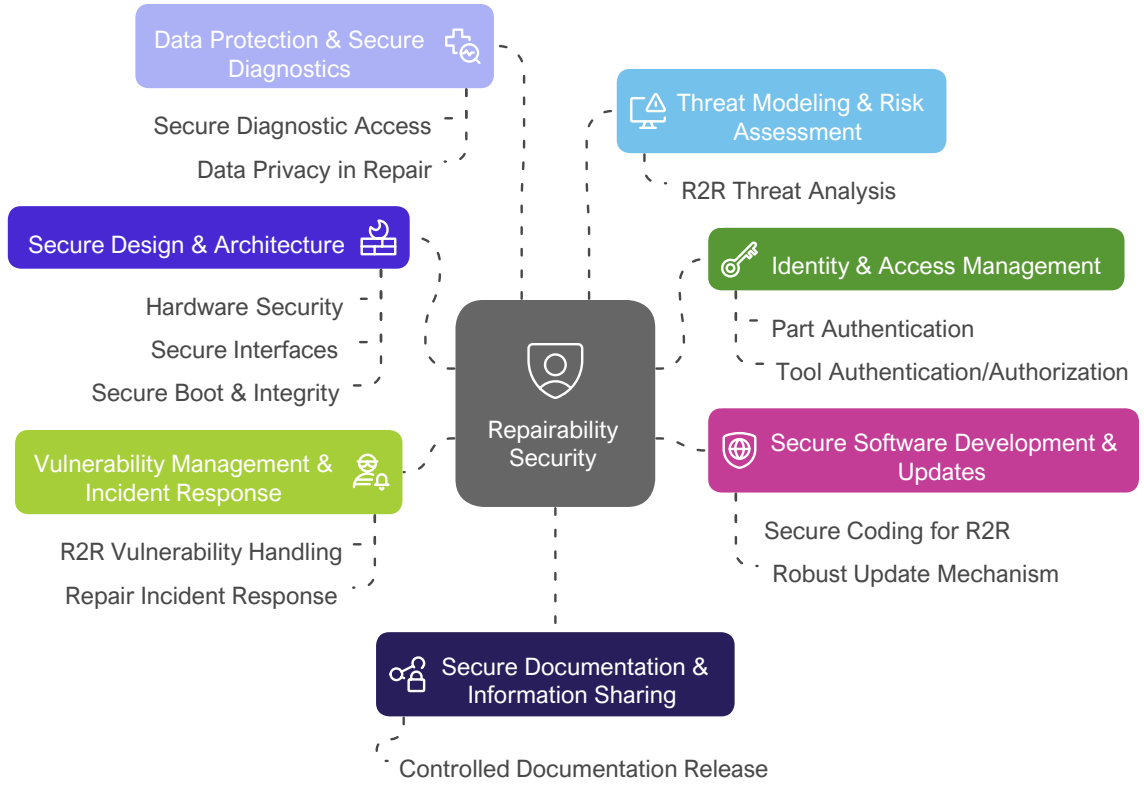
Product Security Management Integration



Product End of Life / Support Considerations

- Document, communicate, and support the full product lifetime
- Support actions beyond patching
- Explore OpenEoX with suppliers
- Communicate via product security management systems
- Coordinate with marketing, sales, services

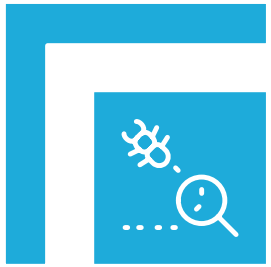
- Balance repairability (R2R) with security and integrity



Trends to Monitor

Model Checker Testing

Formal correctness testing via Alloy, TLA+, and others

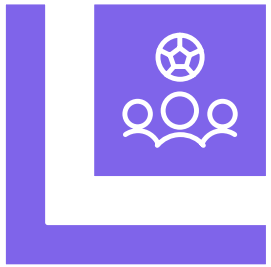


Root of Trust

Secure boot, isolation, cryptographic/trusted services, unique identification, interaction, secure update, etc.

Purple Teaming

Enhance security through collaborative engineering and security testing.



Product-Specific Security

Firmware vulnerability scanners, embedded runtime protection, monitoring and alerting, supply chain management

PIXEL FIRE

Call to action

3 **Guide Behaviors**

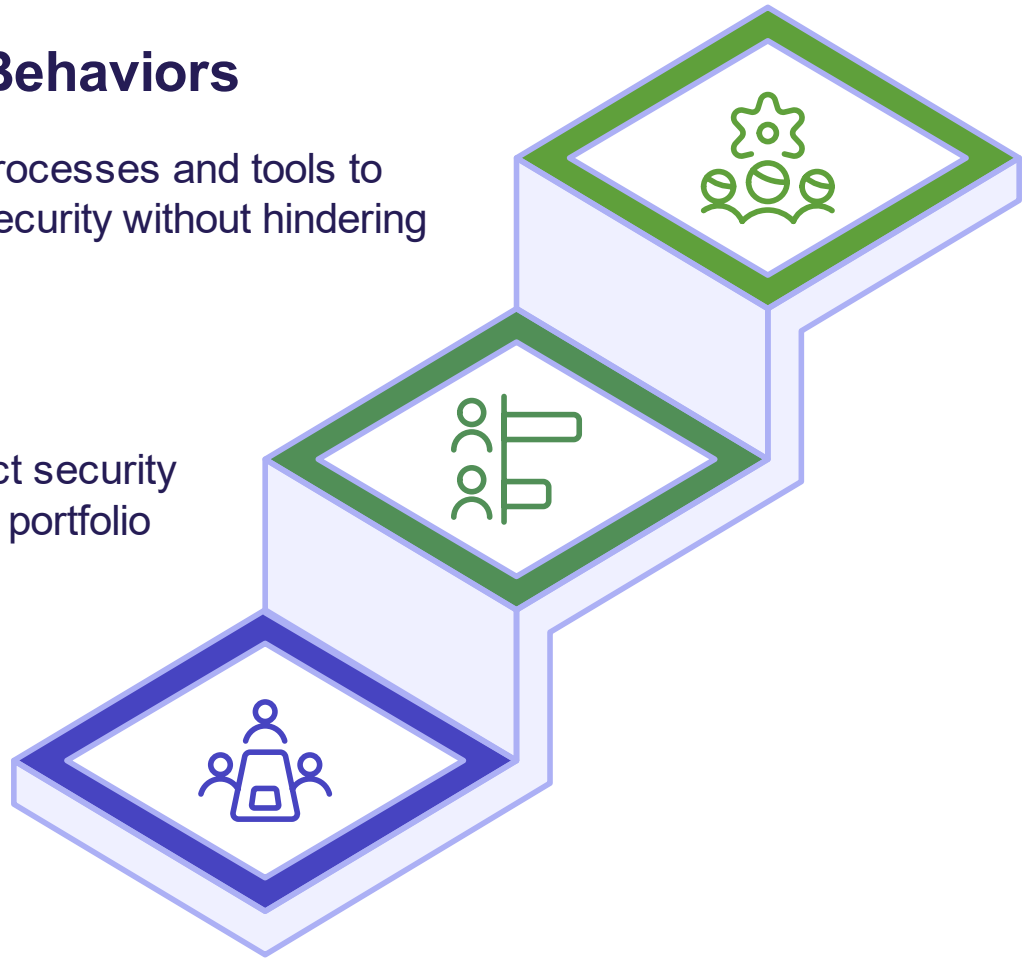
Integrate processes and tools to enhance security without hindering innovation.

2 **Build Team**

Develop a tailored product security team to address specific portfolio needs.

1 **Initiate Change**

Engage executives to secure support and funding for product security initiatives.



RSAC 2025 Conference

Questions

Many Voices.
One Community.

RSAC™ 2025 Conference

Many Voices.
One Community.